

Fig. 3

[k-th TIME AUTHENTICATION PHASE]

PERSON TO BE AUTHENTICATED U_B
(USER ID = A, PASSWORD = S)

AUTHENTICATING PERSON U_A

GENERATE AND STORE RANDOM
NUMBER $N_{(k)}$
 $E_{(k)} \leftarrow E(A, S @ N_{(k)})$
 $E^2_{(k)} \leftarrow E(A, E_{(k)})$
 $E^3_{(k)} \leftarrow E(A, E^2_{(k)})$
 $E_{(k-1)} \leftarrow E(A, S @ N_{(k-1)})$
 $E^2_{(k-1)} \leftarrow E(A, E_{(k-1)})$
 $F_{(k-1)} = E_{(k-1)} @ E^2_{(k-1)} @ E^3_{(k)}$
 $G_{(k)} = E^2_{(k)} @ E^2_{(k-1)}$

INFORM A, $F_{(k-1)}$ AND $G_{(k)}$ IN
A NORMAL ROUTE

$Z' = G_{(k)} @ Z$
 $W \leftarrow E(A, Z')$
 $X = F_{(k-1)} @ Z @ W$
 $Y \leftarrow E(A, X)$

$Y = Z ?$

No

Yes

AUTHENTICATION
IS NOT APPROVED

AUTHENTICATION IS APPROVED
STORE Z' AS NEW
AUTHENTICATION PARAMETER
 Z (FOR THE $k+1$ TIME
AUTHENTICATION) OF U_B

T04240" S0E99Z60

Fig. 4

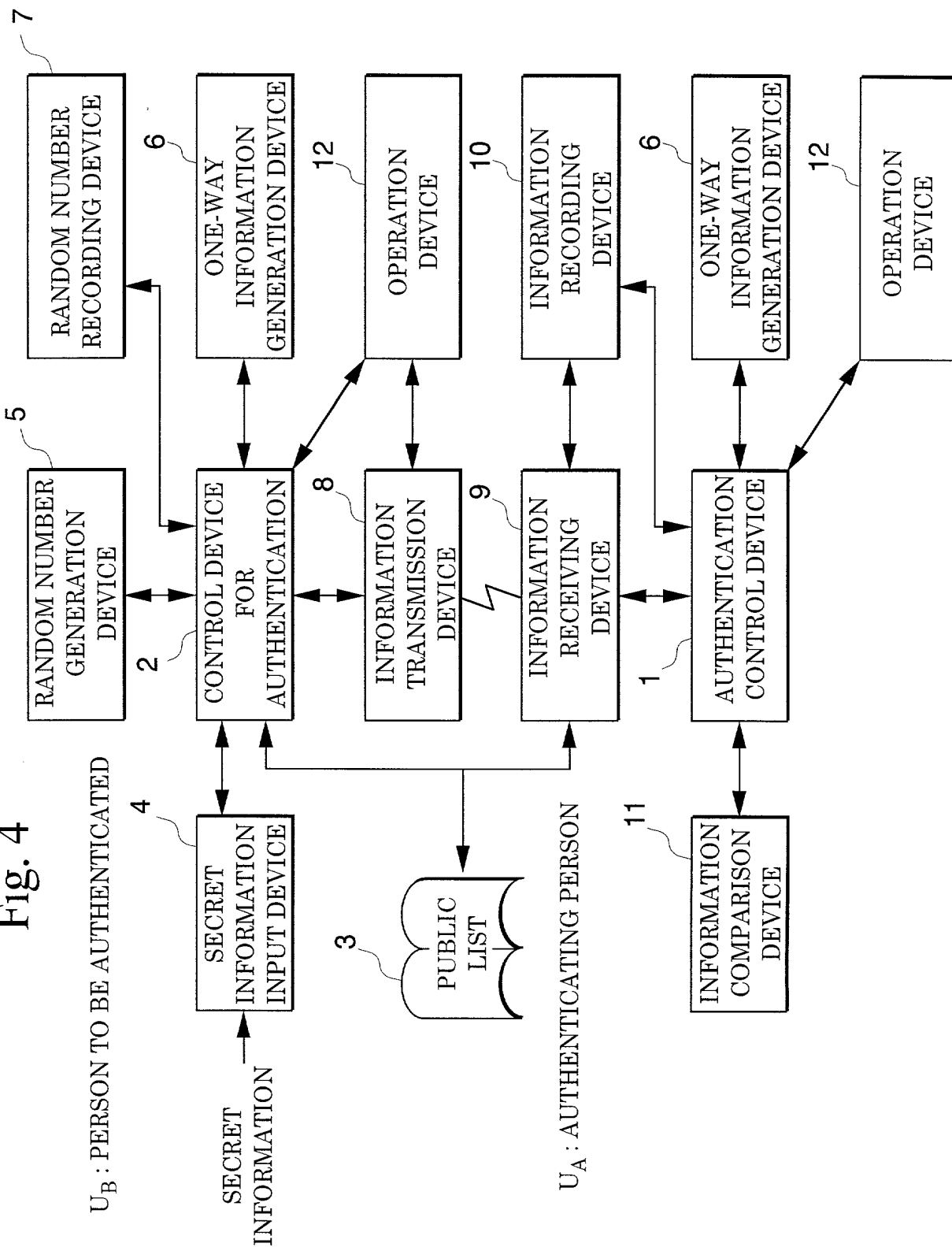


Fig. 2

[INITIAL AUTHENTICATION PHASE]

PERSON TO BE AUTHENTICATED U_B
(USER ID = A, PASSWORD = S)

AUTHENTICATING PERSON U_A

GENERATE AND STORE
RANDOM NUMBER $N_{(1)}$
 $E_{(1)} \leftarrow E(A, S@N_{(1)})$
 $E^2_{(1)} \leftarrow E(A, E_{(1)})$
 $E^3_{(1)} \leftarrow E(A, E^2_{(1)})$
 $E_{(0)} \leftarrow E(A, S@N_{(0)})$
 $E^2_{(0)} \leftarrow E(A, E_{(0)})$
 $F_{(0)} = E_{(0)}@E^2_{(0)}@E^3_{(1)}$
 $G_{(1)} = E^2_{(1)}@E^2_{(0)}$

INFORM A, $F_{(0)}$ AND $G_{(1)}$
IN A NORMAL ROUTE

$Z' = G_{(1)}@Z$
 $W \leftarrow E(A, Z')$
 $X = F_{(0)}@Z@W$
 $Y \leftarrow E(A, X)$

$Y = Z ?$

No

Yes

AUTHENTICATION
IS NOT APPROVED

AUTHENTICATION IS APPROVED
STORE Z' AS NEW
AUTHENTICATION PARAMETER
(FOR NEXT-TIME
AUTHENTICATION) OF U_B

0976305 0740 T04240" 50E99260

Fig. 1

[REGISTRATION PHASE]

PERSON TO BE AUTHENTICATED U_B
(USER ID = A, PASSWORD = S)

AUTHENTICATING PERSON U_A

GENERATE AND STORE
RANDOM NUMBER $N_{(0)}$
 $E_{(0)} \leftarrow E(A, S @ N_{(0)})$
 $E^2_{(0)} \leftarrow E(A, E_{(0)})$

INFORM A, $E^2_{(0)}$
IN A SECURE ROUTE

$Z = E^2_{(0)}$
STORE Z AS AUTHENTICATION
PARAMETER (FOR FIRST-TIME
AUTHENTICATION) OF U_B

09763093460